

AO 93 (Rev. 12/09) Search and Seizure Warrant

| | |
|--|--------|
| ✓ FILED | LODGED |
| RECEIVED | COPY |
| DEC 19 2023 | |
| CLERK U.S. DISTRICT COURT DISTRICT OF ARIZONA | |
| BY <i>dv</i> | DEPUTY |

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

One Apple iPhone 13 Cell Phone
IMEI: 358743274687121

Case No. 23-2983mb

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Arizona

(identify the person or describe the property to be searched and give its location):

As further described in Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

As set forth in Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before

01-02-2024

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.Date and time issued: 12/19/202311:27am

Judge's signature

City and state: Yuma, Arizona

Honorable James F. Metcalf, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

1. The property to be searched is one (1) Apple iPhone 13 smartphone, belonging to Craig MENTA (hereafter the "SUBJECT CELLULAR TELEPHONE"). The SUBJECT CELLULAR TELEPHONE is currently being stored at 7431 E 30th Street, Suite 1, Yuma, AZ 85365 and has so been since the date of incident. This warrant authorizes the forensic examination of the SUBJECT CELLULAR TELEPHONE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. Any records and information found within the digital contents of the SUBJECT CELLULAR TELEPHONE that relate to violations of Title 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance) and Title 21 U.S.C. §§ 952 and 960(a)(1) and (b)(3) (Importation of a Controlled Substance), including:

- a. all information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of drugs or drug packaging;
- b. all information related to buyers or sources of drugs (including names, addresses, telephone numbers, locations, or any other identifying information);
- c. all bank records, checks, credit card bills, account information, or other financial records reflecting the disposition of drug proceeds;
- d. all information regarding the receipt, transfer, possession, transportation, or use of drug proceeds;
- e. any information recording schedule or travel;
- f. evidence of who used, owned, or controlled the SUBJECT CELLULAR TELEPHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, correspondence, and phonebooks;
- g. evidence indicating how and when the SUBJECT CELLULAR TELEPHONE was accessed or used to determine the chronological context of the cellular telephone access, use, and events relating to crime under investigation and to the SUBJECT CELLULAR TELEPHONE user;
- h. evidence indicating the SUBJECT CELLULAR TELEPHONE user’s state of mind as it relates to the crime under investigation;

- i. evidence of the times the SUBJECT CELLULAR TELEPHONE was used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT CELLULAR TELEPHONE;
- k. documentation and manuals that may be necessary to access the SUBJECT CELLULAR TELEPHONE or to conduct a forensic examination of the SUBJECT CELLULAR TELEPHONE;
- l. records of or information about Internet Protocol addresses used by the SUBJECT CELLULAR TELEPHONE to communicate with and/or through “Telegram” or any other communication programs utilized on the SUBJECT CELLULAR TELEPHONE;
- m. records of or information about the SUBJECT CELLULAR TELEPHONE’S Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from “apps,” including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the SUBJECT CELLULAR TELEPHONE.

| | |
|--|---------------------------------|
| <input checked="" type="checkbox"/> FILED | <input type="checkbox"/> LODGED |
| <input type="checkbox"/> RECEIVED | <input type="checkbox"/> COPY |
| DEC 19 2023 | |
| CLERK U.S. DISTRICT COURT DISTRICT OF ARIZONA | |
| BY <i>[Signature]</i> | DEPUTY |

UNITED STATES DISTRICT COURT

for the
District of Arizona



In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
One Apple iPhone 13 Cell Phone)
IMEI: 358743274687121)

Case No. 23-2933mb

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the _____ District of _____ Arizona (identify the person or describe property to be searched and give its location): As further described in Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): As set forth in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 21 U.S.C. § 952, 960, 963, and the application is based on these facts: See attached Affidavit of Special Agent Frank Salcedo

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

FRANK J SALCEDO Digitally signed by FRANK J SALCEDO
Date: 2023.12.19 09:45:22 -07'00'

Applicant's signature

Frank Salcedo, Special Agent, HSI

Printed name and title

Electronically signed and telephonically sworn.

Date: 12/19/2023

City and state: Yuma, Arizona

Judge's signature

Honorable James F. Metcalf, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

1. The property to be searched is one (1) Apple iPhone 13 smartphone, belonging to Craig MENTA (hereafter the "SUBJECT CELLULAR TELEPHONE"). The SUBJECT CELLULAR TELEPHONE is currently being stored at 7431 E 30th Street, Suite 1, Yuma, AZ 85365 and has so been since the date of incident. This warrant authorizes the forensic examination of the SUBJECT CELLULAR TELEPHONE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. Any records and information found within the digital contents of the SUBJECT CELLULAR TELEPHONE that relate to violations of Title 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance) and Title 21 U.S.C. §§ 952 and 960(a)(1) and (b)(3) (Importation of a Controlled Substance), including:

- a. all information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of drugs or drug packaging;
- b. all information related to buyers or sources of drugs (including names, addresses, telephone numbers, locations, or any other identifying information);
- c. all bank records, checks, credit card bills, account information, or other financial records reflecting the disposition of drug proceeds;
- d. all information regarding the receipt, transfer, possession, transportation, or use of drug proceeds;
- e. any information recording schedule or travel;
- f. evidence of who used, owned, or controlled the SUBJECT CELLULAR TELEPHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, correspondence, and phonebooks;
- g. evidence indicating how and when the SUBJECT CELLULAR TELEPHONE was accessed or used to determine the chronological context of the cellular telephone access, use, and events relating to crime under investigation and to the SUBJECT CELLULAR TELEPHONE user;
- h. evidence indicating the SUBJECT CELLULAR TELEPHONE user’s state of mind as it relates to the crime under investigation;

- i. evidence of the times the SUBJECT CELLULAR TELEPHONE was used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT CELLULAR TELEPHONE;
- k. documentation and manuals that may be necessary to access the SUBJECT CELLULAR TELEPHONE or to conduct a forensic examination of the SUBJECT CELLULAR TELEPHONE;
- l. records of or information about Internet Protocol addresses used by the SUBJECT CELLULAR TELEPHONE to communicate with and/or through “Telegram” or any other communication programs utilized on the SUBJECT CELLULAR TELEPHONE;
- m. records of or information about the SUBJECT CELLULAR TELEPHONE’S Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from “apps,” including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the SUBJECT CELLULAR TELEPHONE.

IN THE UNITED STATES DISTRICT COURT
FOR ARIZONA

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE 13 CELL PHONE,
IMEI: 358743274687121, CURRENTLY
LOCATED IN EVIDENCE STORAGE AT
HSI YUMA, 7431 E 30TH STREET, STE 1,
YUMA, AZ 85365

Case No. 23-2933 mb

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent Frank Salcedo, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to examine the cellular telephone described more particularly in Attachment A (hereafter the "SUBJECT CELLULAR TELEPHONE"), and to extract the electronically stored information set forth in Attachment B, which represents evidence and/or instrumentalities of the criminal violations further described below.

2. I am a Special Agent with the Homeland Security Investigations ("HSI") and have been since August 2010. Prior to that, the affiant was a Border Patrol Agent with Customs & Border Protection. The Affiant has a total of approximately 20 years of law enforcement experience. I am currently assigned to the Special Investigations Group, which conducts investigations involving crimes against children, including child pornography as well as other cybernetic crimes. During my employment in law enforcement, I have written and/or participated in the execution of multiple search warrants. The statements contained in this Affidavit are based on my experience and background as a Special Agent and on information provided by other law enforcement agents. I am currently the Computer Forensics Agent (CFA) for my office. I have been the CFA since graduating from the HSI Basic Computer Evidence Recovery training July of 2018. Your Affiant received specific training on how electronic devices, including but not limited to, cellular phones, tablets, and computers of all varieties, to include global positioning system (GPS) devices, can be

used to aid criminals in illegal endeavors. These devices can be used with no security features to take extra steps to thwart law enforcement, to fully customized versions of the devices where readily available and/or custom security steps are taken by criminal elements to add layers of "security" to these devices in an effort to thwart law enforcement and investigative efforts. This training taught your Affiant how to conduct cyber investigations more thoroughly, and forensically sound digital evidence recovery from nearly any type of digital media storage platform from computers and servers to mobile devices such as cellular phones and tablets, as well as drones and gaming consoles, and virtual machines.

3. The statements contained in this Affidavit are based on information derived from the Affiant's personal knowledge, training and experience; information obtained from the knowledge and observations of other sworn law enforcement officers, either directly or indirectly through their reports or affidavits; and surveillance conducted by law enforcement officers.

4. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, your Affiant has not set forth all of the relevant facts known to law enforcement officers.

II. BASIS FOR PROBABLE CAUSE

5. On October 29, 2023, at approximately 4:40 p.m., Craig MENTA (hereinafter "MENTA"), applied for admission into the United States at the San Luis, Arizona Port of Entry via the primary vehicle lanes. MENTA was the driver and sole occupant of a red 2017 Chevy Cruze bearing Arizona license plate number TXA5ZR.

6. MENTA presented an Arizona driver's license and provided a negative verbal customs declaration. During the inspection of the vehicle, Customs and Border Protection Officers ("CBPO") observed a computer-generated alert for the vehicle. The vehicle was then referred to the vehicle secondary lot for further inspection.

7. Prior to entering the secondary lot, the vehicle was scanned by the Z-Portal X-ray machine. Anomalies were observed in the vehicle's trunk area.

8. At the secondary lot, a Canine Enforcement Officer utilized her Hyman and Narcotics Detection Dog ("HNDD") screen the vehicle. The HNDD alerted to the backseat area of the vehicle. A subsequent search of the vehicle revealed a non-factory compartment in the trunk.

Four (4) clear vacuum-sealed packages containing light-blue pills were removed from the trunk. One of the packages was probed and a sample of a blue pills were obtained, which field tested positive for Fentanyl. The 4 packages had a combined net weight of approximately 24.39 kilograms (53.65 pounds).

9. Prior to being interviewed by HSI, MENTA complained to CBP Officers that he was not feeling well and was experiencing chest pain. The San Luis Fire Department (SLFD) was called to provide medical assistance to MENTA. SLFD advised that they would need to transport MENTA to the Yuma Regional Medical Center for proper medical evaluation. MENTA was released pending charges. MENTA was not interviewed by HSI.

10. The SUBJECT CELLULAR TELEPHONE is currently in the lawful possession of HSI. It came into the HSI's possession in the following way: the SUBJECT CELLULAR TELEPHONE was found in MENTA's vehicle on October 29, 2023, during the Customs and Border Protection ("CBP") processing of MENTA during secondary inspection. The SUBJECT CELLULAR TELEPHONE was seized by CBP and then seized by HSI. The SUBJECT CELLULAR TELEPHONE has since been in the custody of HSI. Therefore, while the HSI might already have all necessary authority to examine the SUBJECT CELLULAR TELEPHONE, I seek this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT CELLULAR TELEPHONE will comply with the Fourth Amendment and other applicable laws.

11. The SUBJECT CELLULAR TELEPHONE is currently in storage at HSI Yuma evidence storage at 7431 E 30th Street, Suite 1, Yuma, AZ 85365 since the date of incident, kept in a powered-on state. In my training and experience, I know that the SUBJECT CELLULAR TELEPHONE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT CELLULAR TELEPHONE first came into the possession of HSI.

III. IDENTIFICATION OF THE DEVICE TO BE SEIZED AND EXAMINED

12. The property to be searched is an Apple iPhone 13 seized from MENTA. CBP took the phone from MENTA during his application to enter the United States via the San Luis, Arizona, CBP Port of Entry on October 29, 2023.

13. Based upon the facts contained in this Affidavit, your Affiant submits there is probable cause to believe that the items listed in Attachment B will be found in the contents of the SUBJECT CELLULAR TELEPHONE.

14. Based on my training, education, and experience, and discussions with other trained law enforcement personnel, along with information provided by sources of information and confidential sources, your Affiant knows the following:

a. Drug traffickers commonly use cellular telephones to communicate with other drug traffickers and customers about drug-related activities through the use of telephone calls, text messages, email, chat rooms, social media, and other internet- and application-based communication forums. Moreover, drug traffickers commonly use other capabilities of cellular telephones to further their drug trafficking activities. Therefore, evidence related to drug trafficking activity is likely to be found on the SUBJECT CELLULAR TELEPHONE.

b. Drug traffickers often have access to large amounts of United States currency in order to maintain and finance their ongoing trafficking activities. Therefore, records of the movement of drug proceeds, including deposits, transfers, and purchases, are likely to be found on the SUBJECT CELLULAR TELEPHONE.

15. In addition to items which may constitute evidence and/or instrumentalities of the crimes set forth in this Affidavit, your Affiant also requests permission to seize any articles tending to establish the identity of persons who have dominion and control over the SUBJECT CELLULAR TELEPHONE.

IV. DIGITAL EVIDENCE STORED WITHIN A CELLULAR TELEPHONE

16. As described in Attachment B, this application seeks permission to search for records and information that might be found in the contents of the SUBJECT CELLULAR TELEPHONE. Thus, the warrant applied for would authorize the copying of electronically stored information under Rule 41(e)(2)(B).

17. Probable cause. Your Affiant submits that there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on the SUBJECT CELLULAR TELEPHONE for at least the following reasons:

a. Your Affiant knows that when an individual uses a cellular telephone, the cellular telephone may serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The cellular telephone is an instrumentality of the crime because it is used as a means of committing the criminal offense. The cellular telephone is also likely to be a storage medium for evidence of crime. From my training and experience, your Affiant believes that a cellular telephone used to commit a crime of this type may contain: data that is evidence of how the cellular telephone was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

b. Based on my knowledge, training, and experience, your Affiant knows that cellular telephones contain electronically stored data, including, but not limited to, records related to communications made to or from the cellular telephone, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic "address books;" photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system ("GPS") information.

c. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a cellular telephone, deleted, or viewed via the Internet. Electronic files downloaded to a cellular telephone can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the cellular telephone until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the cellular telephone that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a

cellular telephone's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

18. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the cellular telephone was used, the purpose of the use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be found in the contents of the SUBJECT CELLULAR TELEPHONE because:

a. Data in a cellular telephone can provide evidence of a file that was once in the contents of the cellular telephone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. As explained herein, information stored within a cellular telephone may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the cellular telephone. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the cellular telephone was remotely accessed, thus inculpatory, or exculpatory the owner. Further, activity on a cellular telephone can indicate how and when the cellular telephone was accessed or used. For example, as described herein, cellular telephones can contain information that log: session times and durations, activity associated with user accounts, electronic storage media that connected with the cellular telephone, and the IP addresses through which the cellular telephone accessed networks and the internet. Such information allows investigators to understand the chronological context of cellular telephone access, use, and events relating to the crime under investigation. Additionally, some information stored within a cellular

telephone may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The geographic and timeline information described herein may either inculcate or exculpate the user of the cellular telephone. Last, information stored within a cellular telephone may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how the cellular telephone was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a cellular telephone that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, cellular telephone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one cellular telephone is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

19. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit imaging or otherwise copying the contents of the SUBJECT CELLULAR TELEPHONE, including the use of computer-assisted scans.

20. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

21. Your Affiant submits there is probable cause to believe that the items listed in Attachment B, which constitute evidence and/or instrumentalities Title 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), and Title 21 U.S.C. §§ 952 and 960(a)(1) and (b)(3) (Importation of a Controlled Substance) are likely to be found in the contents of the SUBJECT CELLULAR TELEPHONE further described in Attachment A.

**FRANK J
SALCEDO**

Digitally signed by
FRANK J SALCEDO
Date: 2023.12.19
09:46:09 -07'00'

Special Agent Frank Salcedo
Special Agent
Homeland Security Investigations

Subscribed and sworn to me telephonically this 19th day of December 2023.


HONORABLE JAMES F. METCALF
UNITED STATES MAGISTRATE JUDGE